2022年度

第9回 末松安晴賞贈呈

（写真：敬称略）

本会選奨規程第20条（電子情報通信分野において，学術，技術，標準化などにおいて特に顕著な貢献が認められ，今後の進歩・発展が期待される）に基づき，下記の2件を選び贈呈した．

学術界貢献

次世代共通鍵暗号の研究開発と社会展開

受賞者 **五十部孝典**

五十部孝典君は，2006年に神戸大学工学部，2008年に同大学院自然科学研究科修士課程，2013年に同博士課程を修了した．2008年からソニー株式会社に入社し，2017年まで務めた．2017年4月から兵庫県立大学大学院情報科学研究科の准教授として着任，2023年4月に同教授に昇進し，現在に至っている．

同君はこれまで，「IoT向け暗号」と「Beyond 5G向け暗号」の実装要求の極めて厳しい環境向けの新世代暗号を世界に先駆けて開発した．関連論文は，暗号分野のトップ会議や論文誌に40本以上採録され，その引用数も2,000件を超えており，当該分野を世界的にけん引し学術的に多大な貢献をしている．IoT機器向けの暗号として，低回路規模暗号PiccoloとWARP，低消費電力暗号Midoriなどの軽量暗号アルゴリズムを開発した．PiccoloとWARPは，暗号演算で求められる非線形関数を論理ゲートレベルから最適化を図ることで回路規模を標準暗号AESの約1/5の600 GEに削減した．2023年現在，回路規模としては世界最小である．またMidoriでは，漏れ電流の影響を考慮し消費電力を最小化する理論モデルを構築し，AESと比較して消費電力を1/10にすることに成功した．これも2023年現在，低消費電力性能では世界一の性能を持つ．また，Beyond 5G向け暗号として超高速暗号Roccaと低遅延暗号Orthrosを開発した．Roccaは，ソフトウェアで高速に実行可能な命令のみから暗号を構成するアプローチを取り，ソフトウェアでの大幅な高速化を実現した．結果として，Beyond 5Gの要件であるソフトウェアで100 Gbit/s超のスループットと量子コンピュータへの安全性を世界で初めて達成した．ソフトウェアでの暗号化速度としては，AESの5倍以上あり，現在世界最速の暗号である．Orthrosは，演算に必要な遅延の小さいコンポーネントを最適に組み合わせて構成することで演算遅延の最小化を図っている．結果として，AESの1/3以上の低遅延性能で，Beyond 5G時代のリアルタイム暗号化としての要件であるサブナノ級の低遅延での暗号化を世界で初めて達成した．

以上のとおり，同君の電子情報通信分野における貢献は顕著であり，本賞を受賞するにふさわしいと考える．同君の研究の更なる進展と今後の活躍に期待する．

産業界貢献

パスワードレス個人認証の研究開発，国際標準化および商用化

受賞者　**大神　涉**

大神　涉君は，2010 年に九州大学工学部電気情報工学科を卒業後，2012 年に京都大学大学院情報学研究科知能情報学専攻修士課程を修了し，ヤフー株式会社に入社した．入社後は主に Yahoo! JAPAN 研究所で，ユーザ環境情報を用いたユーザビリティとセキュリティ並びにパスワードレス認証技術の研究開発に従事してきた．

同君は，パスワードレス個人認証技術の開発・国際標準化・事業化に対する貢献が顕著である．同君は，単一認証器を前提とした FIDO（Fast Identity Online）のパスワードレス認証プロトコルを複数認証器にもパスワードレスで適用できるように拡張した．具体的には，FIDO 準拠の複数認証器パスワードレス登録方法と認証方法を提案・実装・動作検証し，安全性を評価した．前記登録方法は，デバイス内と外の利用可能認証器数及び認証器間の個人認証済証明データ転送方法に対応した 4 典型例に対応する．また，前記認証方法は，利用者側ブラウザの機能とサービス提供 Web サイトで安全のために必要な条件の組合せ 7 種類に対応する．更に，前記認証方法に基づいて，利用者デバイス紛失等によって喪失したアカウントアクセス権を短時間で簡単に回復できる，アクセス権回復方法を開発した．これらは FIDO の認証プロトコル自体ではないが，商用化に欠かせない実用必須技術である．これらの詳細技術・実装・安全性評価結果を FIDO 標準化へ還元し，主著者として FIDO 白書を執筆した．国内では，サブグループ共同座長として，FIDO 技術の周知，関係者の意見集約等を主導した．Yahoo! JAPAN（YJ）サービス認証サーバの FIDO 認定（2015 年），同 FIDO2 対応認証サーバの FIDO 認定（2018 年），Android 端末向け（2018 年）/iOS 端末向け（2020 年）FIDO2 対応 YJ 認証サービス導入と常に世界初でシステムを開発し，商用化を達成した．更に同君は，YJ 社内認証ゲートウェイに FIDO 認証を導入するプロジェクトをマネージャとして統括し，2019 年 12 月に導入を実現した．YJ サービスは 2022 年 9 月現在までに累計 1,750 万人以上が利用しており，YJ 社内認証ゲートウェイは 2019 年 12 月から約 270 人が，Android/iOS のスマートホンと Windows/macOS の PC から利用している．

このように，パスワードレス個人認証技術及び FIDO 標準化に対する同君の貢献は顕著であり，本会末松安晴賞にふさわしいものである．